KRYPTERA ACCELERATES PRODUCT DEVELOPMENT OF THE MIRAGE REAL-TIME MASS ENCRYPTION SERVER

Kryptera has developed a real-time mass encryption turnkey server called Mirage that allows organizations to rapidly protect their private files. In their project, Kryptera tested the mass encryption and decryption speed of Mirage on a CENGN server, and across a network.

SECURITY AND PERFORMANCE NEEDS

Organizations across a wide range of industries have an extensive amount of small to large digital assets that need to be encrypted in case of a serious cyber breach. There are several security products on the market that can encrypt individual smaller files with low latency and retrieval times, but no key management solutions that can mass encrypt files of any size as efficiently as Mirage. For organizations with stronger encryption requirements, processing speed is a concern as users need to quickly store and retrieve files at the highest possible speeds.

AN ADDED LAYER OF SECURITY

Kryptera Mirage mass encryption technology has the power to rapidly handle small to large file sizes, and complex directories. But it is especially useful for organizations requiring encryption of bulky files that are hundreds of GB in size, such as database backups or uncompressed 4K videos.

Kryptera's Mirage solution was developed to address the requirements of organizations that need to manage the retention and transport of multiple types of sensitive files.

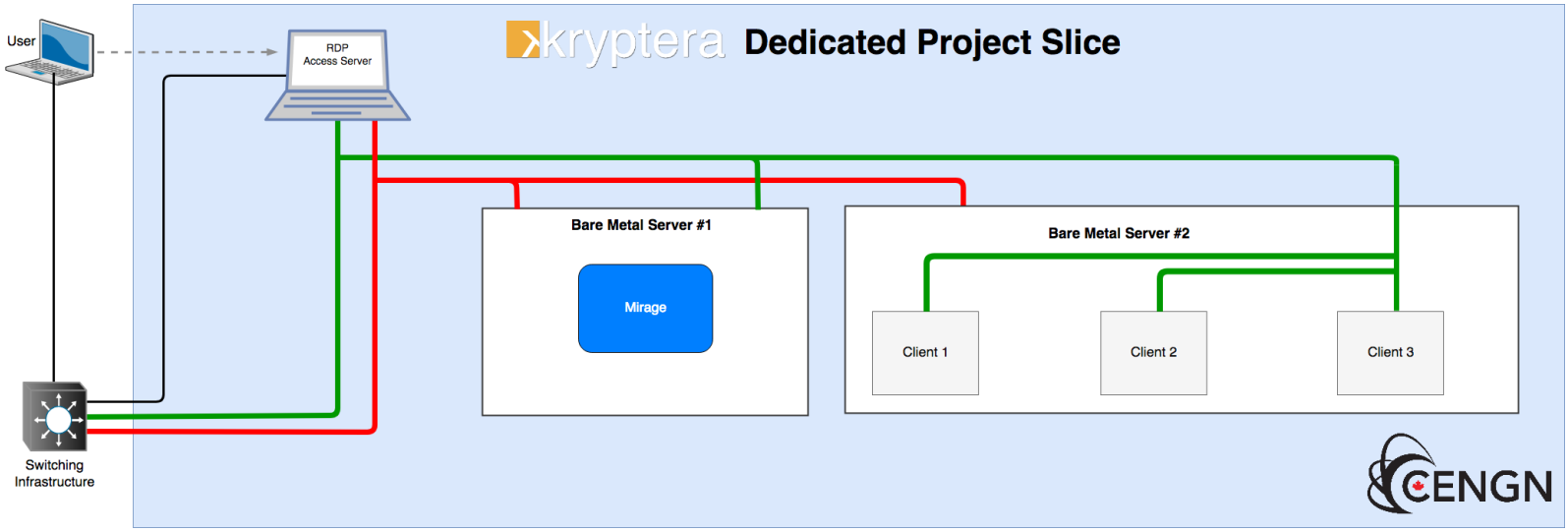
Mirage ensures that confidential private files are securely encrypted and can only be decrypted by select users and automated processes within the organization.

Mirage adds an important layer of defense. Even if a data breach does occur and an intruder, trusted employee, or contractor gains access to a company's servers and computers, files that have been encrypted by Mirage cannot be viewed or utilized in any way by unauthorized users.

CENGN TESTING

To prepare for taking Mirage to market, Kryptera needed to test the performance and stability of Mirage in a computing environment similar to what a prospective customer would have. CENGN offered the network services for Kryptera to achieve this.

The Mirage project had three goals; identify any issues in the encryption and decryption process, optimize performance, and establish processing benchmarks that can be provided to potential customers. Mirage was also tested and benchmarked against the OpenSSH server encrypting files using AES-NI by Intel®.



CENGN MEMBERS

Bell · Cisco · EXFO · Huawei · Invest Ottawa | Investir Ottawa · Juniper Networks · Mitel Powering connections · Nokia · ribbon · Rogers · TELUS · WIND

TEST RESULTS

Test Phase 1: Configuration and Local File System Testing.

After Mirage was shown to be operational on a bare metal server, files ranging in size from 10 MB to 300 GB were created and stored on the local file system, then moved to the rapid mass encryption server for processing. During the process the system was powered down during encryption and decryption to confirm that files could be recovered with processing correctly completed. Kryptera's fastest server-side processing time for Mirage was a blazing 1.63 billion bytes/second when decrypting 12 files at 25 GB in size.

Test Phase 2: Remote File Setup

Next up, clients 1-3 were installed on bare metal server #2, which acted as a remote file system. This represented traffic being sent from one to three remote servers for encryption and decryption.

Test Phase 3: Remote Speed and Robustness

Custom software was developed to:

1. automate the creation of files that ranged from 10 MB to 200 GB,
2. time multi-threaded file transfers to and from Mirage across the network, and
3. do discretionary verification of source files with associated decrypted files.

Mirage processed files as quickly as possible using all available threads. The combined speed was recorded for transferring all files across the network to Mirage, and then waiting for each file to be either encrypted or decrypted before transferring it back to the client.

The fastest client-server processing time for Mirage was 482.5 million bytes/second when encrypting 1,000 files at 100 MB in size. Transferring files to and from the server reached about 1.34 billion bytes/second across the 10gbit network.

Compared to the speed of server-side file processing, transferring files to and from the server across the network for a complete encryption or decryption cycle significantly slowed the speed of file processing.

Test Phase 4: Product Enhancements

With the technical help of CENGN, Kryptera made improvements to the Mirage encryption server software and ran test cases. This was done to prove that there were no missing files after processing 100,000 files that ranged in size from 10-15 MB.

TAKEAWAYS

Kryptera was able to take away important lessons from the CENGN project and improve their solution in the following ways:

- Kryptera was able to enhance the Mirage software to improve client-server processing performance by 400%;
- Kryptera determined that liquid cooled servers and the use of Graphics Processing Units (GPUs) will significantly increase Mirage's encryption/decryption speed;
- Kryptera added a file detection feature to ensure no files are lost in the encryption/decryption process;
- Kryptera determined that their Mirage encryption server was 4x faster than the OpenSSH server encrypting files using AES-NI by Intel® largely due to its mass encryption feature;
- Kryptera determined the Mirage solution can run on the latest Ubuntu LTS OS.

CONCLUSION

The CENGN project produced sterling results for Kryptera, demonstrating that Mirage mass encryption and decryption can easily and efficiently handle very large files such as videos or database backups.

The testing at CENGN also demonstrated that Mirage technology can be useful for real-time encryption and decryption of data and voice streams between secure nodes without need of passing a private key. The strength of Mirage encryption ensures that encrypted streams can be passed through an insecure network connection without any security risk.

CENGN
CENTRE OF EXCELLENCE IN NEXT GENERATION NETWORKS

CENGN

Rick Penwarden, Marketing Manager
rick.penwarden@cengn.ca
cengn.ca/projects

Alastair Sweeny, VP, Business Development
asweeny@kryptera.ca
kryptera.ca

kryptera